Ex Let ξ be an n^{th} root of unity in $\mathbb{C}$, i.e. $\xi^n = 1$. Then $G(\mathbb{Q}(\xi)/\mathbb{Q})$ is abelian, in fact a subgroup of $\mathbb{Z}_n^*$.

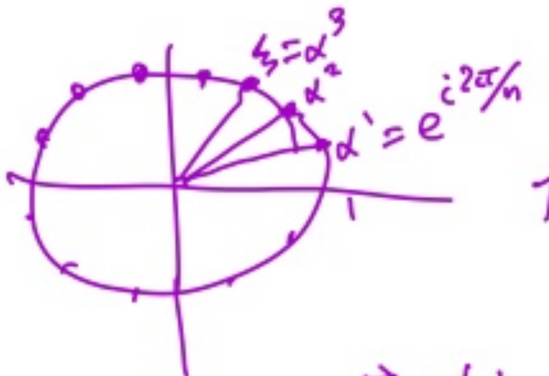
Pf. Since $\xi^n = 1$, $\text{irr}(\xi, \mathbb{Q})$ is an irreducible factor of $x^n - 1$. If $\xi = \alpha^r$, where $\alpha = e^{2\pi i/n}$, $r < n$

What are the other roots of this factor of $x^n - 1$?

If we wish to calculate $[\mathbb{Q}(\xi) : \mathbb{Q}]$, we see the basis must be $1, \xi, \xi^2, \dots, \xi^{k-1}$, where $k = \deg(\xi, \mathbb{Q})$.

$\Rightarrow 1, \alpha^r, \alpha^{2r}, \dots, \alpha^{(k-1)r}$ is a basis.

Further, $1, \alpha^r, \alpha^{2r}, \dots, \alpha^{kr}$ is linearly dependent.



Let's compute $[\mathbb{Q}(\alpha) : \mathbb{Q}]$.

The roots are all α^k for some k — evenly spaced around the circle.

$$\Rightarrow 1 + \alpha + \alpha^2 + \dots + \alpha^{n-1} = 0$$

$$0 = 1 - \alpha^n = (1-\alpha)(1 + \alpha \dots + \alpha^{n-1}) = 0$$

Suppose $\phi \in G(\mathbb{Q}(\alpha)/\mathbb{Q})$.

$\phi(\alpha) =$ another root of unity $= \alpha^s$ for some $s \in \{1, \dots, n-1\}$

(In fact, if ϕ is any isomorphism of $\mathbb{Q}(\alpha) \to E$, it must be of this form, since splitting field S of $x^n - 1$ is normal & sep.). Also, α generates the splitting field, because all the roots are α^s.

Given any automorphism $\psi \in G(S/\mathbb{Q})$, ψ must be of the form ψ_{α,α^s}.

We define a map $F: G(S/\mathbb{Q}) \to \mathbb{Z}_n^*$

by $\psi_{\alpha,\alpha^s} \mapsto s$ $\quad F(\psi_{\alpha,\alpha^s}) = s \bmod n$

Let's check that it's a group isomorphism:

$$F(\psi_{\alpha,\alpha^s} \circ \psi_{\alpha,\alpha^t}) = F(\psi_{\alpha,\alpha^{ts}}) = ts$$

$\alpha \mapsto \alpha^t \mapsto (\alpha^t)^s = \alpha^{ts}$

$$= F(\psi_{\alpha,\alpha^t})\, F(\psi_{\alpha,\alpha^s}) =$$

$$= F(\psi_{\alpha,\alpha^s})\, F(\psi_{\alpha,\alpha^t}).$$ Thus it is a homomorphism.

$$\operatorname{Ker} F = \{\psi_{\alpha,\alpha^s} : F(\psi_{\alpha,\alpha^s}) = 1 \in \mathbb{Z}_n^*\}$$

$$= \{\psi_{\alpha,\alpha^s} : s \equiv 1 \bmod n\} = \{\psi_{\alpha,\alpha}\} = Id.$$

$\therefore$ it is 1-1.

Also, it is onto, since $\forall\, m \in (\mathbb{Z}^n)^*$,

$$F(\psi_{\alpha,\alpha^m}) = m.$$

$\therefore$ F is an isomorphism.

We have show $G(S/\mathbb{Q}) \cong \mathbb{Z}_n^*$,

where S is the splitting field of $x^n - 1$.

We are trying to calculate $G(\mathbb{Q}(\xi):\mathbb{Q})$:

The argument is similar.

<u>Define</u> $u\left(\psi_{\alpha^r,\alpha^{rs}}\right) \in \mathbb{Z}_m^*$ by

$$u: G(\mathbb{Q}(\xi)/\mathbb{Q}) \to \mathbb{Z}_m^*$$

by $\left(\psi_{\alpha^r,(\alpha^r)^s}\right) \longmapsto s$

where $m = \text{minimum}\{s > 0 : rs \equiv 0 \bmod n\}$

$(m|n)$, so $\mathbb{Z}_m^*$ is a subgroup of $\mathbb{Z}_n^*$.

$\therefore$ $G(\mathbb{Q}(\xi)/\mathbb{Q})$ is abelian.

<u>Fact</u>. If E is a Galois extension of F that is finite, then it is a simple extension, $E = F(\alpha)$, so that E is the splitting field of $\mathrm{irr}(\alpha, F)$. Since every element of $G(E/F)$ must map roots of $\mathrm{irr}(\alpha, F)$ to themselves,

$G(E/F) \cong$ a subgroup of S_n, where

$n = [E:F] = \deg(\alpha, F)$.

(This is only true if α = a primitive element.)

Thm. Let E be a finite extension of a finite field F of order p^n.
Then $G(E/F)$ is cyclic and generated by the Frobenius automorphism

$$\sigma_{p^n}(\alpha) = \alpha^{p^n}.$$